



Cyber Security

How To Protect Your Business & Yourself

Sejal Lakhani-Bhatt – CEO TechWerxe

TECHWERXE

We can **MONITOR THE DARK WEB** for you
\$178/Month

For all BTA Attendees
Call Sejal at 973-577-4548 and mention BTA.

Call TechWerxe for:
Security Solutions
Cybersecurity Training for Employees
Cybersecurity Seminars

TECHWERXE

Expectations and Disclaimer

- What we will cover:
 - Multi-Layered Cyber Security Strategy
 - Cyber Security Awareness
- What we will not cover:
 - Any Politics
 - Football
- Goal for Today:
 - Improve knowledge about cyber scams
 - Know what tricks the hackers are using so you won't fall for their next one
 - Not end up in a situation where we're running an IT fire drill or where we've compromised sensitive information

TECHWERX

~A Little History & Why This Is Important ~



- 556 Million victims is the number of REPORTED attacks each year
- Approximately \$103 billion in funds is stolen globally each year

TECHWERX

By The Numbers

- Cost of avg. attack on SMBs:
 - \$8,699 in 2013
 - \$20,752 in 2014
 - \$36,000 in 2016
- 33% of firms required 3+ days to recover from attack
- 60% SMBs fail within 6 months of being hacked

By the numbers

- 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster and 50% filed for bankruptcy immediately
- 20 % of small to medium business will suffer a major disaster causing loss of critical data every 5 years
- About 70 % of business people have experienced data loss due to accidental deletion, disk or system failure, viruses, fire or some other disaster
- 40% of small to medium businesses that manage their own network and use the internet , will have their network accessed by the hackers, and more than 50 % wont even know they were attacked

Sources: Ponemon; Symantec; Nat'l Small Bus. Assoc.

TECHWERX

Scam of the Week

Scam of the Week: Equifax Phishing Attacks

You already know that a whopping 143 million Equifax records were compromised. The difference with this one is that a big-three credit bureau like Equifax tracks so much personal and sometimes confidential information like social security numbers, full names, addresses, birth dates, and even drivers licenses and credit card numbers for some.

It can be the difference between being able to buy a house or sometimes even get a job or not. This breach and the way they handled it, including the announcement, was what Brian Krebs rightfully called a dumpster fire.

The problem is that with this much personal information in the hands of the bad guys, highly targeted spear phishing attacks can be expected, and a variety of other related crime like full-on identity theft on a much larger scale.

These records are first going to be sold on the dark web to organized crime for premium prices, for immediate exploitation, sometimes by local gangs on the street. Shame on Equifax for this epic fail. They will be sued for billions of dollars for this web-app vulnerability.

So this Scam of the Week covers what is inevitable in the near future, we have not seen actual Equifax phishing attacks at this point yet, but you can expect them in the coming days and weeks because the bad guys are going to take their most efficient way to leverage this data... email.

I suggest you send the following to your employees, friends, and family. You're welcome to copy, paste, and/or edit:

**Cyber criminals have stolen 143 million credit records in the recent hacking scandal at big-three credit bureau Equifax. At this point you have to assume that the bad guys have highly personal information that they can use to trick you. You need to watch out for the following things:*

- Phishing emails that claim to be from Equifax where you can check if your data was compromised
- Phishing emails that claim there is a problem with a credit card, your credit record, or other personal financial information
- Calls from scammers that claim they are from your bank or credit union
- Fraudulent charges on any credit card because your identity was stolen



TECHWERX



Printer Vulnerabilities Expose Organizations to Attacks

By Eduard Kovacs on January 30, 2017

[Share](#)
[210](#)
[G+](#)
[Twitter](#)
[Facebook](#)
[Recommend 34](#)
[RSS](#)

A team of researchers from Ruhr-Universität Bochum in Germany has analyzed 20 printers and multifunction printers (MFPs) from several vendors and discovered that each of them is affected by at least one vulnerability, including flaws that can be exploited to crash the device or obtain sensitive information that provides access to the organization's network.

The experts conducted their tests on printers from HP, Brother, Lexmark, Dell, Samsung, Konica, Oki and Kyocera using a Python-based piece of software they named PRinter Exploitation Toolkit (PRET). The analysis revealed the existence of both old and new vulnerabilities and attack vectors that can be exploited locally or remotely.

Some of the attack methods detailed by the researchers involve what they call PostScript malware. PostScript, created more than 30 years ago by Adobe, is a computer language used to describe the appearance of text and graphics on a page. The language is supported by all major printer manufacturers.

According to researchers, an attacker can abuse PostScript to manipulate documents, such as in the attack where thousands of printers were hijacked and made to print anti-Semitic flyers, or to capture the content of documents that are printed.

Such attacks can be launched through USB, remotely over the local network, or from the Internet via a malicious website using cross-site printing (XSP) and cross-origin resource sharing (CORS) spoofing.

Experts also showed how PostScript and Printer Job Language (PCL) can be leveraged to access the entire file system on some printers, including passwords for the embedded web server. This vulnerability has been known for several years, but experts say it still hasn't been completely fixed.

"OKI MC342dn allows an attacker to execute one level of path traversal, where a directory called 'hidden/' is located which contains stored fax numbers, email contacts and local users' PINs as well as the SNMP community string," researchers said in their paper. "More interesting, however, is the fact that this MFP can be integrated into a network using features like Email-to-Print or Scan-to-FTP. An attacker could find passwords for LDAP, POP3, SMTP, outbound HTTP proxy, FTP, SMB, and Webdav as well as the IPsec pre-shared keys. This is a good example how an attacker can escalate her way into a company's network, using the printer device as a starting point."



Is salutation consistent for sender?

Can you spot any other warning signs?

From: John Smith [mailto:john.smith@abcsteelworks.com]
Sent: Wednesday, April 27, 2016
To: Susan Jones
Subject: Payment Needed Today!

Susan - Are you available to make urgent payment for me today?

John M. Smith, President and CEO
T: 555-555-1111 e: john.smith@abcsteelworks.com

From: Susan Jones [mailto:susan.jones@abcsteelworks.com]
Sent: Wednesday, April 27, 2016
To: John Smith
Subject: RE: Payment Needed Today!

Yes, I am in the office all day. Please send me the payment details.

Susan Hoyle
Controller/CFO
T: 555-555-2222 e: susan.jones@abcsteelworks.com

From: John Smith [mailto:john.smith@abcsteelworks.com]
Sent: Wednesday, April 27, 2016
To: Susan Jones
Subject: RE: Payment Needed Today!

Attached are payment instructions. Code to Admin Expenses. I am out and not reachable by cell today use email only. Let me know as soon as payment sent - must be done today or we pay big late fee.


John M. Smith, President and CEO
T: 555-555-1111 e: john.smith@abcsteelworks.com

Fake domain:
replaced 'w' with 'vv' (two v's)

Real domain has 'w'

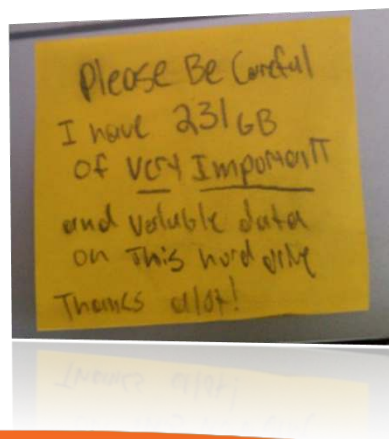
Other examples of domain name alterations:

- l vs. i or 1
- q vs. g
- 0 vs. O
- rn vs. m
- Extra/missing letters
abcsteellworks.com
abcsteelwork.com



Helpful Tip #1: Backup Your Data

1. Run Daily Backups of Critical Data
2. Automated Offsite Backups Are Invaluable
3. Check / Test Your Data Backups Monthly (Minimum)



TECHWERX

Helpful Tip #2: Password Rules

- DON'T SHARE PASSWORDS
 - This includes your "IT Guy"
 - Type your password for them
- One Password Per Account
- No Password POST-IT NOTES!
- Change Your Password Every 60 Days
- Use a phrase with numbers and characters:

"I Only Have Eyes For You"

➡ "!0hE4uAug"

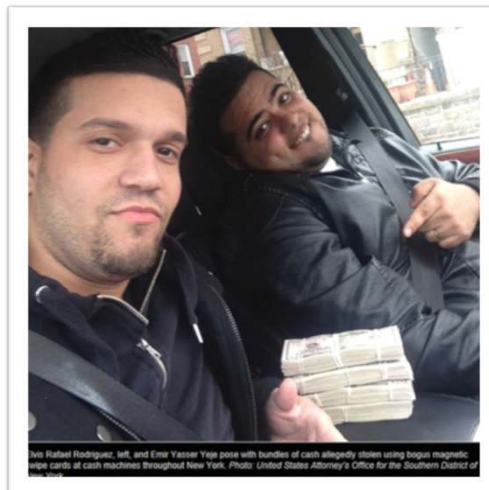
And here's the list of the 10 most hacked passwords, of hacked Yahoo! accounts, according to ESET.

1. '123456' used by 1666 (0.38%)
2. 'password' used by 780 (0.18%)
3. 'welcome' used by 436 (0.1%)
4. 'ninja' used by 333 (0.08%)
5. 'abc123' used by 250 (0.06%)
6. '123456789' used by 222 (0.05%)
7. '12345678' used by 208 (0.05%)
8. 'sunshine' used by 205 (0.05%)
9. 'princess' used by 202 (0.05%)
10. 'qwerty' used by 172 (0.04%)

TECHWERX

Helpful Tip #3: What To Do If Attacked

- Disconnect Your Workstation From The Network AND Internet
- Seek Professional Help
- When Appropriate, Contact The Police And Your Insurance Company
- Don't Start "Googling" For The Fix
 - Russian firm w/ 500 employees wrote the bug and charged \$79.95 to your credit card to fix the solution they created in the first place!



TECHWERX

Government Guidance: Put better locks on your door

Leadership & IT Professionals

- Implement Defense-in-Depth: a layered defense strategy includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your system's anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all of your software.
- Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.

Report a computer or network vulnerability to the
U.S. Computer Emergency Readiness Team;

Incident Hotline: 1-888-282-0870
www.US-CERT.gov



Homeland
Security

For more cyber tips and resources, visit the Department of
Homeland Security's Stop.Think.Connect.™ Campaign at:
www.dhs.gov/stopthinkconnect



STOP | THINK | CONNECT™

TECHWERX

Phishing Email Awareness

- Most phishing emails try to simulate a daily task or invoke a strong emotional reaction
- Think twice about any email that makes you feel strongly about anything financial
- Good anti-spam systems filter out 99% of all phishing emails
- Education on computer and email security can help with the remaining 1%

TECHWERX

Helpful Tip #4: Common Sense Security

- Train Staff On Social Engineering!
- Know The Source
- Limit Telephone Information Sharing
- Physical Security
- Wireless "Hot Spots" & Hotel Internet
- Your Equipment @ Offsite Locations including Starbucks & Conferences
- Ability To Disable The Device If It's Lost Or Stolen (LoJack, Encryption, Etc.)



TECHWERX

Helpful Tip #5: Advanced Security Tips

- Don't Use "Home" Version of Microsoft Windows On Your Company Workstations
- Encrypt Your Hard Drive
- Use Email Hygiene Provider / Service
- Use Server Based Group Policies
- Use MSP to Manage Company Firewall(s)
- Establish Company-wide Data Policies



TECHWERX



TECHWERX

Sejal Lakhani-Bhatt/ CEO

973-577-4548

slakhani@techwerxe.com

Call us for all your security solutions!

The logo for TechWerxe features the word "TECH" in a grey, sans-serif font, followed by "Werxe" in a stylized orange font where the 'W' and 'e' are connected. A thin orange arc is positioned above the text, and a thick black arc is positioned below it.

TECHWerxe™